#2

S/N Filed Herewith

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Jung Jin PARK	Examiner:	Unknown
Serial No.:	Filed Herewith	Group Art Unit:	Unknown
Filed:	Filed Herewith	Docket No.:	13424.7US01
Title:	DEVICE AND METHOD FOR SCRAMBLING/DESCRAMBLING VOICE AND DATA FOR MOBILE COMMUNICATION SYSTEM		

CERTIFICATE UNDER 37 CFR 1.10

'Express Mail' mailing label number: EL674897480US
Date of Deposit: November 21, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents and Trademarks, Washington, D.C. 20231.

By: Brant Miles
Name: Brant Miles

SUBMISSION OF PRIORITY DOCUMENT(S)

Box: New App.
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Applicants enclose herewith one certified copy of a Republic of Korea application, Serial No. 1999-58711, filed December 17, 1999, the right of priority of which is claimed under 35 U.S.C. § 119.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(612) 332-5300

Dated: November 21, 2000

By Curtis B. Hamre
Curtis B. Hamre
Reg. No. 29,165

CBH/kas

#2

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 1999년 제 58711 호
Application Number

출 원 년 월 일 : 1999년 12월 17일
Date of Application

출 원 인 : 현대전자산업주식회사
Applicant(s)

2000 년 10 월 30 일

특 허 청
COMMISSIONER

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0002

【제출일자】 1999.12.17

【발명의 명칭】 이동통신 시스템에서의 음성 및 데이타 암호화/복호화장치 및 그 방법

【발명의 영문명칭】 Method and apparatus for scrambling/descrambling a voice/data in a mobile communication system

【출원인】

【명칭】 현대전자산업 주식회사

【출원인코드】 1-1998-004569-8

【대리인】

【성명】 문승영

【대리인코드】 9-1998-000187-5

【포괄위임등록번호】 1999-000829-7

【발명자】

【성명의 국문표기】 박정진

【성명의 영문표기】 PARK,JUNG JIN

【주민등록번호】 671108-1101713

【우편번호】 467-860

【주소】 경기도 이천시 부발읍 아미리 산 136-1

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
문승영 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	12	면	12,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	15	항	589,000 원
【합계】	630,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명에 따른 이동통신 시스템의 음성/데이타를 암호화/복호화하기 위한 장치 및 그 방법은 무선채널구간에서 전송되어온 신호를 보코딩 또는 바이패스시킨 후, 보코딩 또는 바이패스된 신호를 랜덤넘버를 이용하여 스크램블링하여 유선채널 구간으로 전송하고, 유선채널 구간으로 부터 수신되는 스크램블링된 신호를 동기신호의 검출 유무에 따라 상기 랜덤넘버에 따라 디스크램블링한 후, 보코딩 또는 바이패스시켜 무선채널 구간으로 전송하는 것으로서, 기존의 상용 이동통신 시스템에서 추가적인 하드웨어 변경없이 소프트웨어의 변경만으로 구현 가능한 장점이 있으며, 시스템 보코더간 유선채널 구간에서의 보안성을 획기적으로 유지시켜 도청을 미연에 방지할 수 있도록 한 것이다.

【대표도】

도 4

【명세서】

【발명의 명칭】

이동통신 시스템에서의 음성 및 데이타 암호화/복호화장치 및 그 방법 {Method and apparatus for scrambling/descrambling a voice/data in a mobile communication system}

【도면의 간단한 설명】

도 1은 일반적인 이동통신 시스템에서 이동 가입자간의 통화시 채널 구간별 전송형태를 나타낸 도면,

도 2는 일반적인 이동통신 시스템에서 보코더 바이패스된 패킷 유형을 나타낸 도면으로서, 도 2a는 바이패스된 음성 패킷의 포맷을 나타낸 도면이고, 도 2b는 바이패스된 데이타 패킷의 포맷을 나타낸 도면,

도 3은 종래 기술에 따른 이동통신 시스템에서의 동작 모드별 보코딩 장치의 블록 구성을 나타낸 도면,

도 4는 본 발명에 따른 이동통신 시스템에서의 음성 및 데이타 암호화/복호화장치의 블록 구성을 나타낸 도면,

도 5는 본 발명에 따른 이동통신 시스템에서 음성 및 데이타 암호화/복호화방법에 대한 동작 플로우챠트를 나타낸 도면.

〈도면의 주요부분에 대한 부호의 설명〉

30 : 상위 프로세서 40 : 보코더

41 : 동작모드 처리부 42 : 제어부

43, 48, 50 : 스위칭부 44 : 동기정보 전송부

45 : 암호화시드부 46 : 랜덤넘버 발생부

47 : 스크램블링 49 : 동기신호 검출부

51 : 디스크램블링

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<13> 본 발명은 이동 통신시스템에서의 음성 및 데이타 보코딩에 관한 것으로서, 특히 디지탈 이동통신 시스템의 보코딩 장치에서 이동가입자간 음성 통화 및 데이타 통신 시 시스템내 보코더의 동작 모드에 관계없이 유선채널상의 통신신호를 암호화 및 복호화하기 위한 이동통신 시스템에서 음성 및 데이타 암호화/복호화장치 및 그 방법에 관한 것이다.

<14> 일반적으로, 디지탈 이동통신 시스템에서 제한된 무선채널 용량내에 많은 수의 가입자를 수용하기 위해 음성을 압축하여 전송한다. 음성을 압축하기 위해서는 음성 부호화 알고리즘을 사용하야 하는데, 일반적으로 이동통신 분야에서는 저전송률이면서 유선망 음질을 갖는 보코딩(Vocoding) 알고리즘을 사용한다. 보코딩 알고리즘은 오차가 있는 알고리즘이어서 압축과 복원을 반복하면, 할 수록 복원된 음성과 원음성간의 오차는 커진다. 즉, 복원된 음성의 음질이 저하되는 것이다.

<15> 도 1은 일반적인 이동통신 시스템에서 이동가입자간의 통화시 채널 구간별 전송형

태를 나타낸 도면으로서, 도 1에 도시된 바와 같이, 특히 이동가입자간의 통화일 때, 이동국(1, 1')에서 음성을 압축하여 패킷형태로 전송국(2, 2')에 전송하면, 전송국 시스템 내의 보코더(미도시)에서 전송된 패킷을 PCM(Pulse Code Modulation)형태로 복원한다. 이 복원된 PCM데이타는 교환국(3)을 거쳐 통화하고자 하는 상대편 이동국(1', 1)이 서비스 받고 있는 전송국(2', 2)으로 보내어지고, 다시 전송국(2', 2)내에 있는 보코더에서 재 압축을 한다. 여기서, 상기한 전송국(2, 2')은 제어국과 기지국을 포함한 것이다.

<16> 이렇게 압축된 패킷은 무선채널을 통해 이동국(1', 1)으로 전송된다.

<17> 마지막으로 패킷을 수신한 이동국(1, 1')은 이동국(1, 1')내의 보코더에서 패킷을 복원하게 되고, 이동가입자는 상대방의 음성을 들을 수 있다. 결국, 2회의 보코딩과정을 거치게 됨을 알 수 있다. 그래서 이동가입자간의 통화일 경우 이동국(1, 1')에서 압축되어 무선채널로 전송되어 온 음성패킷을 시스템내에 있는 보코더에서 패킷 바이패스(Packet Bypass)를 시킴으로써, 보코딩 과정을 줄이게 되며, 결국 음질저하를 보완할 수 있다. 또 패킷 바이패스 기능은 데이타 통신시에도 사용된다. 여기서, 이동국(1, 1')과 전송국(2, 2')간은 무선채널구간이고, 전송국(2,2')과 교환국(3)간은 유선채널 구간이다.

<18> 이하, 도 2를 참조하여 종래 기술에 따른 음성신호의 보코딩장치에 대하여 살펴보기로 하자.

<19> 도 2는 일반적인 이동통신 시스템에서 보코더 바이패스된 패킷 유형을 나타낸 도면으로서, 도 2a는 바이패스된 음성 패킷의 포맷을 나타낸 도면이고, 도 2b는 바이패스된 데이타 패킷의 포맷을 나타낸 도면이고, 도 3은 종래 기술에 따른 이동통신 시스템에서의 동작 모드별 보코딩 장치의 블록 구성을 나타낸 도면이다.

<20> 먼저, 이동통신 시스템에서의 보코딩 장치는 보코더(20)와, 상위 프로세서(10)로 이루어진다. 여기서, 상위 프로세서(10)는 전송국(2, 2')과 교환국(3)전체에서 보코더(20)를 제외한 나머지 부분을 총괄하는 부분이다.

<21> 그리고, 상기 보코더(20)는 제 1, 2, 3, 4 모드 스위칭부(22, 26, 27, 31)와, 각 모드별로 보코딩을 처리하는 제 1 내지 제 6 보코딩 처리부(23, 24, 25, 28, 29, 30)로 구성된다.

<22> 이와 같은 구성을 갖는 종래 기술에 따른 이동통신 시스템의 보코딩장치는 이동가입자간 통화시 3가지 모드로 동작한다.

<23> 첫 번째 모드는 통화하고자 하는 이동가입자 단말기내의 보코더가 서로 다른 종류의 보코더인 경우 예를들면, EVCR(Enhanced Variable Code Rate)과 QCELP(Qualcomm Code Excited Linear Predictive)간, 8Kbps QCELP와 13Kbps QCELP간 일 때로 시스템의 보코더는 정상적인 보코딩(음성 부호화와 복호화)과정을 수행한다. 이때, 무선채널(단말기와 시스템 보코더간 전송로)상에서는 패킷 형태로 통신되며, 유선채널(교환국을 사이에 둔 시스템 보코더간 전송로)상의 전송형태는 PCM이다.

<24> 두 번째모드는 통화하고자 하는 이동가입자 단말기의 보코더가 서로 동일할 경우로, 예를들면, EVCR과 EVCR 또는 QCELP와 QCELP일 때로 시스템의 보코더는 음성 패킷 바이패스(Voice Packet Bypass)모드로 동작한다. 이때에는 무선채널상에서 패킷 형태로 주고 받으며, 유선채널상에서의 전송형태는 도 2a에 도시된 바와 같은 바이패스된 음성 패킷이다.

<25> 그리고, 세 번째 모드는 이동가입자간 데이타 통신을 할 경우로서 시스템 보코더는

데이타 패킷 바이패스(Data Pcket Bypass)모드로 동작한다. 이때, 무선채널구간은 패킷 형태로 주고 받으며, 유선채널 구간은 도 2b와 같은 바이패스된 데이타 패킷 형태로 전송한다.

<26> 이와 같이 상기한 세가지 모드로 동작을 수행하는 보코딩 시스템은 도 3에 도시되었다.

<27> 도 3에서 보듯이 보코더(20)는 상위 프로세서(10)로 부터 3가지 모드중 한가지의 모드로 동작할 수 있는 모드 정보(E)를 받아서 모드 제어기(21)에서 각 모드에 맞는 동작을 제어하고, 즉, 상위 프로세서(10)로 부터 상기한 첫 번째 모드 정보가 입력되면, 모드 제어기(7)는 스위칭부(22, 26)를 제 1 보코딩 처리부(23)로 스위칭하여 이동단말기에서 무선채널(A)을 통해 전송되어 온 음성 패킷을 PCM으로 보코딩하여 PCM데이타를 교환국으로 유선채널(C)을 통해 전송한다. 또한, 모드 제어기(21)는 스위칭부(27, 31)를 제 4 보코딩 처리부(28)로 스위칭시켜 교환국에서 유선 채널(D)을 통해 전송한 PCM데이타를 패킷 데이타로 보코딩하여 무선채널(B)을 통해 통화하고자 하는 이동단말기로 전송하는 것이다.

<28> 한편, 상위 프로세서(10)로 부터 상기한 두 번째 모드 정보가 입력되면, 모드 제어기(7)는 스위칭부(22, 26)를 제 2 보코딩 처리부(24)로 스위칭하여 이동단말기에서 무선채널(A)을 통해 전송한 음성 패킷을 바이패스시켜 바이패스된 음성 패킷 데이타를 유선채널(C)을 교환국으로 전송한다. 또한, 모드 제어기(21)는 스위칭부(27, 31)를 제 5 보코딩 처리부(29)로 스위칭하여 교환국에서 유선 채널(D)을 통해 전송된 음성패킷 데이타를 바이패스시켜 바이패스된 음성 패킷 데이타를 무선채널(B)을 통해 통화하고자 하는 이동단말기로 전송하는 것이다.

<29> 또한, 상위 프로세서(10)로 부터 상기한 세 번째 모드 정보가 입력되면, 모드 제어기(7)는 스위칭부(22, 26)를 제 3 보코딩 처리부(23)로 스위칭하여 이동단말기에서 무선채널(A)을 통해 전송된 데이타 패킷을 바이패스시켜 바이패스된 데이타 패킷을 교환국으로 유선채널(C)을 통해 전송되도록 한다. 또한, 모드 제어기(21)는 스위칭부(27, 31)를 제 6 보코딩 처리부(30)로 스위칭하여 교환국에서 유선 채널(D)을 통해 전송한 데이타 패킷을 바이패스시켜 바이패스된 데이타 패킷을 무선채널(B)을 통해 통화하고자 하는 이동단말기로 전송하는 것이다.

<30> 상기한 바와 같이 보코더(20)는 상위 프로세서(10)와 모드 정보 뿐 만 아니라 무선채널(A, B)상을 통신하는 패킷을 주고 받으며, 보드 정보에 따라 적절한 처리과정을 수행하며, 유선채널(C, D)구간으로는 모드에 따라 도 2에 도시된 형태와 같은 바이패스된 패킷 및 PCM등을 입출력한다. 그리고, 상위 프로세서(10)는 보코더(20)를 제어하는 역할뿐 아니라 무선채널을 통해 이동국과 시스템 보코더간의 패킷 통신을 하게 해준다.

<31> 이와같은 종래 기술에 따른 보코딩 시스템에서 시스템 보코더가 상기한 각 모드로 동작할 때, 특히 유선 채널상에서 도청이 쉽게 될 수 있는 문제점이 잇다. 즉, 보코딩 모드로 동작할 경우 즉, 상기 첫 번째 모드로 동작할 경우 유선 채널구간에서 전송되는 PCM은 도청장비에 의해 쉽게 도청할 수 있다.

<32> 그리고, 두번 째 모드 즉, 음성 패킷 바이패스 모드로 동작할 경우로 일반 PCM도청방법으로는 도청할 수 없으나, 도 2a에서 보듯이 순수 음성 패킷이 미리 정의된 필드에 정해진 순서대로 위치하고 있기 때문에 바이패스된 음성 패킷전체에서 음성 패킷을 찾을 수 있는 위치에 대한 경우의 수는 매우 제한적이어서 쉽게 도청당할 수 있는 것이다.

<33> 또한, 상기와 유사하게 세번 째 모드 즉, 데이타 패킷 바이패스 모드에서도 도 2b

에 도시된 바와 같이 바이패스된 데이타 패킷이 유선채널상에서 반복적으로 나타날 것이며, 동일한 패턴을 가지는 플래그 필드(Flag Field)를 제거하고 나면 쉽게 수순 데이타 패킷을 추출해 낼 수 있는 것이다.

【발명이 이루고자 하는 기술적 과제】

<34> 따라서, 본 발명은 상기한 문제점을 해결하기 위하여 안출한 것으로 본 발명의 목적은 전송측 시스템 보코더내에 암호화기능을 두어 유선채널상으로 전송하고자 하는 통신신호를 암호화하여 전송하고, 수신측 시스템 보코더내에는 암호화된 데이타를 복호화할 수 있는 해독기능을 두어 통신신호를 해독할 수 있도록 한으로써, 도청을 방지할 수 있도록 한 이동통신 시스템에서의 음성 및 데이타 암호화 복호화장치를 제공함에 있다.

<35> 또한, 본 발명의 다른 목적은 상기한 보코딩장치의 동작과 상응하는 음성 및 데이타 암호화/복호화방법을 제공함에 있다.

<36> 결국, 본 발명은 유선 채널구간에서 음성 도청 및 데이타의 유출을 막기위해 보안성을 높일 필요가 있다. 따라서, 시스템 보코더내에 암호화기와 해독기를 모두 설치하여 상위 프로세서로부터 제공되는 동일한 암호화키를 이용하여 통신신호를 암호화하고 수신되는 암호화된 통신신호를 해독할 수 있도록 한 이동통신 시스템에서의 음성 및 데이타 암호화/복호화딩 장치 및 그 방법을 제공함에 있다.

<37> 상기한 목적을 달성하기 위한 본 발명에 따른 이동통신 시스템에서의 음성 및 데이타 암호화장치의 특징은 무선채널 구간으로 부터 전송되어 온 음성/데이타 패킷을 제공

되는 동작 모드신호에 따라 보코딩하거나 바이패스시키는 동작 모드 처리부와; 공급되는 암호화키에 따라 랜덤넘버를 발생시키는 랜덤넘버 발생부와; 제공되는 제어신호에 따라 동기신호를 발생하여 유선채널 구간으로 전송하는 동기신호 전송부와; 상기 랜덤넘버 발생부에서 발생된 랜덤넘버를 이용하여 상기 동작 모드 처리부에서 보코딩 또는 바이패스된 PCM 또는 음성/데이타패킷을 암호화한 후, 상기 동기신호의 전송이 완료되면, 유선채널 구간으로 전송하는 암호화부와; 상기 동작 모드 제어신호, 암호화키 공급 제어신호 및 상기 동기신호 발생 제어신호를 제공하는 제어부로 구성됨에 있다.

<38> 또한, 본 발명에 따른 이동통신 시스템에서 음성 및 데이타 복호화장치의 특징은 유선채널 구간으로 부터 전송되어 온 암호화된 신호에서 동기신호를 검출하는 동기신호 검출부와; 제공되는 복호화키에 따라 랜덤넘버를 발생하는 랜덤넘버 발생부와; 제공되는 복호화 제어신호에 따라 상기 랜덤넘버 발생부에서 발생한 랜덤넘버에 따라 유선채널로 부터 수신된 암호화된 신호를 복호화하는 복호화부와; 상기 동기신호 검출부에서 동기신호가 검출되면, 상기 복호화부에 복호화 제어신호를 제공하고, 상기 복호화키를 공급할 수 있도록 제어신호를 제공하는 제어부와; 제공되는 동작모드에 따라 상기 복호화부에서 복호화된 PCM을 보코딩하여 패킷으로 변환하거나 또는 음성/데이타 패킷을 그대로 바이패스시킨 후, 무선채널 구간으로 전송하는 동작 모드 처리부로 구성됨에 있다.

<39> 또한, 본 발명에 따른 이동통신 시스템에서 음성 및 데이타 암호화/복호화장치의 특징은 무선채널 구간으로 부터 전송되어 온 음성/데이타 패킷을 제공되는 동작 모드신호에 따라 보코딩하거나 바이패스시키고, 복호화된 PCM 또는 패킷을 제공되는 동작 모드에 따라 보코딩 또는 바이패스시켜 무선채널 구간으로 전송하는 동작 모드 처리부와; 공급되는 암호화 및 복호화키에 따라 랜덤넘버를 발생시키는 랜덤넘버 발생부와; 제공되는

제어신호에 따라 동기신호를 발생하여 유선채널 구간으로 전송하는 동기신호 전송부와; 상기 랜덤넘버 발생부에서 발생된 랜덤넘버를 이용하여 상기 동작 모드 처리부에서 보코딩 또는 바이패스된 PCM 또는 음성/데이타패킷을 암호화한 후, 상기 동기신호의 전송이 완료되면, 유선채널 구간으로 전송하는 암호화부와; 유선채널 구간으로 부터 전송되어 온 암호화된 신호에서 동기신호를 검출하는 동기신호 검출부와; 제공되는 복호화 제어신호에 따라 상기 랜덤넘버 발생부에서 발생한 랜덤넘버에 따라 유선채널로 부터 수신된 암호화된 신호를 복호화하는 복호화부와; 상기 동기신호 검출부에서 동기신호가 검출되면, 상기 복호화부에 복호화 제어신호를 제공하고, 상기 암호화키 및 복호화키를 공급할 수 있도록 제어신호를 제공하고, 상기 동기신호 발생 제어신호를 제공하는 제어부로 구성됨에 있다.

<40> 또한, 본 발명에 따른 이동통신 시스템에서의 음성 및 데이타 암호화방법의 특징은 무선채널 구간에서 전송되어온 음성 패킷 또는 데이타 패킷을 제공되는 동작 모드에 따라 보코딩 또는 바이패스시킨 후, 출력하는 단계와; 제공되는 암호화키 정보에 따라 임의의 일정한 랜덤 넘버를 발생하는 단계와; 제공되는 제어신호에 따라 동기신호를 발생하여 발생된 동기신호를 유선채널 구간으로 전송하는 단계와; 상기 동기신호가 전송되면 상기 발생한 랜덤 넘버를 이용하여 상기 모드 처리된 신호(PCM 또는 바이패스된 음성패킷 또는 바이패스된 데이타 패킷)을 암호화한 후, 암호화된 신호를 유선채널구간으로 전송하는 단계로 이루어짐에 있다.

<41> 또한, 본 발명에 따른 이동통신 시스템에서 음성 및 데이타 복호화방법의 특징은 유선채널 구간으로 부터 암호화된 신호를 수신하는 단계와; 암호화된 신호가 수신되면,

수신된 암호화된 신호에서 동기신호를 검출하는 단계와; 동기신호가 검출되면, 제공되는 복호화키에 의해 임의의 일정한 랜덤넘버를 발생하는 단계와; 상기 발생된 랜덤넘버에 의해 상기 수신된 암호화된 신호를 복호화하는 단계와; 상기 복호화된 PCM 또는 패킷을 제공되는 동작모드에 의해 보코딩 또는 바이패스시켜 패킷으로 변환한 후, 무선채널구간으로 전송하는 단계로 이루어짐에 있다.

【발명의 구성 및 작용】

<42> 이하, 본 발명에 따른 이동통신 시스템에서의 음성/데이타 암호화/복호화장치 및 그 방법에 대하여 첨부한 도면을 참조하여 상세하게 살펴보기로 한다.

<43> 먼저, 본 발명은 상기 종래 기술에서 설명한 바와 같이 이동가입자간 통화시 보코더의 동작모드에 따라 유선 채널구간에서 전송되는 통신신호의 유형은 모두 3가지 이다. 즉, 음성통화시 보코더가 보코딩 모드로 동작할 경우 PCM이고, 음성 패킷 바이패스 모드로 동작할 경우에는 바이패스된 음성 패킷이다.

<44> 그리고, 데이타 통신시에는 보코더는 데이타 패킷 바이패스모드로 동작하며, 유선 채널구간에서 바이패스된 데이타 패킷 형태이다. 이와 같은 모든 유형에 대하여 암호화 및 복호화가 가능하도록 하기 위한 것이다.

<45> 도 4는 본 발명에 따른 이동통신 시스템에서의 음성/데이타를 암호화하고 해독하는 보코딩 시스템의 블록 구성을 나타낸 도면으로서, 도 4를 참조하여 그 구성을 살펴보면, 동작모드 정보 및 암호화키 정보를 제공하는 상위 프로세서(30)와, 상위 프로세서(30)에서 제공되는 모드 정보에 따라 입력되는 단말기에서 무선채널(A)을 통해 전송한 음성 또

는 데이타 패킷을 보코딩 또는 바이패스모드로 동작 처리하고, 디스크램블링된 신호를 패킷으로 보코딩하거나 또는 바이패스모드로 동작 처리하여 패킷을 무선채널(B)을 통해 이동단말기로 전송하는 동작 모드 처리부(41)와, 상위 프로세서(30)에서 제공하는 암호화키 정보를 저장 및 저장된 암호화키정보를 출력시키기 위한 제어신호, 동기신호 전송 제어신호 및 스위칭 제어신호를 각각 발생하여 제공하는 제어부(42)와, 제어부(42)에서 제공되는 저장 제어신호에 따라 상위 프로세서(30)에서 제공되는 암호화키 정보를 저장하고, 출력 제어신호에 따라 저장된 암호화키 정보를 출력하는 암호화키 시드(Seed)부(45)로 구성된다.

<46> 또한, 제어부(42)에서 제공되는 제어신호에 따라 일반모드 또는 암호화모드로 스위칭 전환하는 제 1 스위칭부(43)와, 암호화키 시드부(45)에서 제공되는 암호화키 정보에 따라 랜덤 넘버(Random Number)를 발생시키는 랜덤 넘버 발생부(46)와, 랜덤 넘버 발생부(46)에서 발생된 랜덤 넘버에 따라 동작 모드 처리부(41)를 통해 모드 처리(보코딩 또는 바이패스)된 패킷 또는 PCM신호를 스크램블링(Scrambling)하는 스크램블링부(47)와, 제어부(42)에서 제공되는 동기 신호 전송제어신호에 따라 동기신호를 발생하여 발생된 동기신호를 전송하는 동기신호 전송부(48)와, 상기 동기신호 전송부(49)에서 전송된 동기신호를 먼저 전송하고, 스크램블링부(47) 출력단으로 스위칭하여 스크램블링부(47)에서 스크램블된 신호를 스위칭하여 암호화된 데이타를 유선채널(C)을 통해 교환국으로 전송하는 제 2 스위칭부(48)로 구성된다.

<47> 또한, 유선채널(D)을 통해 수신되는 암호화된 신호에서 동기신호를 검출하는 동기신호검출부(49)와, 동기신호 검출부(49)에서 동기신호가 검출되면, 제어부(42)의 제어신호에 따라 일반모드에서 해독모드로 스위칭전환하는 제 3 스위칭부(50)와, 제 3 스위칭

부(50)의 스위칭에 따라 수신된 암호화된 신호를 디스크램블링(Descrambling)한 후, 상기 동작모드 처리부(41)로 출력하는 디 스크램블링부(51)로 구성된다.

<48> 이와 같은 구성을 갖는 본 발명에 따른 이동통신 시스템에서의 음성/데이타 암호화/복호화장치의 상세 동작에 대하여 설명해 보기로 하자.

<49> 보코더(40)는 상위 프로세서(30)로 부터 동작 모드(E) 및 암호키 정보(F)를 받는다. 그러면, 보코더(40)의 동작모드처리부(41) 및 제어부(42)에서 제어신호를 만드는데 사용되는데, 제어부(42)는 암호키를 암호화 시드부(45)에 저장시킨 후, 저장된 암호화키를 리드하여 랜덤 넘버 발생부(46)로 출력시킨다. 이때, 제어부(42)는 제 1 스위칭부(43)를 a단에서 g단으로 스위칭 전환시키게 된다.

<50> 그리고, 랜덤 넘버 발생부(46)는 암호키 시드부(45)에서 제공되는 암호화키에 따라 임의의 랜덤 넘버를 발생하여 스크램블링부(47)로 제공한다.

<51> 따라서, 스크램블링부(47)는 제 1 스위칭부(43)의 스위칭 전환에 따라 동작모드처리부(41)에서 출력되는 바이패스된 패킷 또는 보코딩된 PCM신호를 랜덤 넘버 발생부(46)에서 제공되는 랜덤넘버에 따라 스크램블 즉, 암호화시킨 후, 제 2 스위칭부(48)로 출력한다. 이때, 제어부(42)는 동기신호 전송부(49)에 제어신호를 제공함과 동시에 제 2 스위칭부(48)에 스위칭 제어신호를 제공하여 동기신호 전송부(49)에서 발생된 동기신호를 유선채널구간으로 먼저 전송하고, 동기신호가 전송되면, 제어부(42)는 제 2 스위칭부(48)를 스크램블링부(47)단으로 스위칭 전환시켜, 스크램블링부(47)에서 암호화된 신호를 유선채널구간으로 전송하게 되는 것이다. 이때, 동기신호는 최초 프레임에 대한 암호화된 신호르 유선채널 구간으로 전송하기 전에 한번만 전송하게 되고, 그 이후의 모든 프레임에 대햐서는 동기신호를 전송하지 않게 된다.

<52> 한편, 유선 채널구간에서 상기와 같이 암호화된 데이타가 수신되면, 보코더(40)의 동기신호 검출부(49)에서는 수신된 암호화된 신호에서 동기신호를 검출하여 동기신호 검출결과를 제어부(42)로 제공한다.

<53> 이때, 제어부(42)는 동기신호 검출부(49)에서 동기신호가 검출되면, 제 3 스위칭부(50)를 d단에서 i단으로 스위칭전환시킨다.

<54> 따라서, 수신된 암호화된 즉, 스크램블링된 신호는 스크램블링의 역과정 즉, 랜덤 넘버 발생부(46)에서 출력되는 랜덤 넘버에 따라 해독되는 것이다. 이렇게 해독된 패킷 또는 PCM신호는 동작모드 처리부(41)로 제공된다.

<55> 동작 모드 처리부(41)는 상위 프로세서(30)에서 제공되는 동작 모드에 따라 보코딩 또는 바이패스 동작을 수행하여 바이패스된 패킷 또는 보코딩된 PCM을 무선채널 구간으로 전송하게 되는 것이다.

<56> 상기한 암호화 및 복호화기능에 대하여 좀 더 상세하게 살펴보기로 하자.

<57> 보코더(40)는 상위 프로세서(30)로 부터 동작모드 및 암호화키 정보를 받는다. 그러면, 보코더(40)는 이정보들로 동작모드처리부(41) 및 제어부(42)에서 제어신호를 만드는데 사용하는데, 제어부(42)는 암호키를 암호화 시드부(45)에 저장시킨 후, 저장된 암호화키를 랜덤넘버 발생부(46)로 출력시킨다. 따라서, 랜덤넘버 발생부(46)는 암호화 시드부(45)에서 제공되는 암호화키에 의해 랜덤넘버를 발생시킨다. 이때, 랜덤 넘버는 보코더(40) 입출력 통신신호를 암호화하거나 해독하는 정보로 사용된다. 이 정보는 보코더(40)의 입출력 통신신호의 위치 정보에 해당되며, 암호화를 수행하는 스크램블링부(47)와 해독을 수행하는 디스크램블링부(51)로 각각 입력된다.

<58> 스크램블링부(47)는 랜던 넘버 발생부(46)에서 발생된 위치정보를 이용하여 동작모드 처리부(41)에서 출력된 통신신호(g)의 각 위치를 비트 또는 바이트단위로 재배열한다. 이때, 암호화의 정도는 암호화하고자 하는 통신신호를 바이트단위로 재배별하는 것보다는 비트단위로 재배열하는 것이 더욱 성능이 뛰어나다. 이렇게 재배열된 신호(h)를 스크램블링부(47)는 동기신호 전송부(49)에서 발생된 동기신호와 합성되어 보코더(40) 출력단(C)로 출력함으로써, 암호화된 신호가 유선채널상으로 전송되는 것이다.

<59> 그리고, 디스크램블링부(51)는 유선채널구간에서 전송되어온 암호화된 신호(D)를 랜덤넘버 발생부(46)에서 발생된 위치 정보를 이용해서 상기 표 1의 스크램블링 과정의 역 과정으로 신호를 역 배열함으로써, 원래의 신호(j)를 해독해내는 것이다. 이 과정에 대한 예를 아래의 표 1을 참고하여 설명해 보자.

<60> 【표 1】

원 위치	0	1	2	3	4	5	6	7	8	9
통신 신호	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9
랜덤 넘버	1	3	5	7	2	9	8	4	6	0
재 배열 된 신호	X1	X3	X5	X7	X2	X9	X8	X4	X6	X0

<61> 설명의 편의상 10바이트 단위로 통신신호(g)를 재 배열(암호화)하고자 한다면, 0 - 9사이의 10개의 랜덤넘버(k)를 발생시킨다. 상기의 표 1과 같이 임의의 랜덤 넘버가 발생하였다면, 첫 번째 랜덤넘버가 1이기 때문에 1의 위치에 있는 통신신호, X1을 첫 번째 위치(위치0)에 가져온다. 그리고, 두 번째 랜덤넘버가 3이기 때문에 3의 위치에 있던

통신신호 X3을 두 번째 위치(위치1)에 가져온다. 이런 방법으로 해서 마지막 아홉 번째 랜덤넘버는 0이기 때문에 0의 위치에 있는 통신신호 X0을 위치(위치9)로 이동시킨다. 결국, 이와 같이 하면 제일 아래의 재 배열된 신호가 얻어지게 되고, 암호화된 신호를 얻을 수 있는 것이다.

<62> 해독과정(디스크램블링)은 상기한 암호화과정을 역으로 수행하면, 쉽게 원래의 통신신호를 역배열할 수 있음을 알 수 있다.

<63> 그런데, 시스템의 전송측과 수신측의 각 보코더가 암호화된 신호를 정확히 해독하기 위해서는 암호화 및 해독을 시작하는 시점이 일치해야 한다. 즉, 시스템 보코더간 유선채널 구간에서 통신신호의 전송지연에 대해 고려해야 한다. 이를 해결하는 방법으로 여러가지가 있을 수 있는데, 시스템의 설계 및 형상에 따라 달라질 수 있다. 여기서는 어떠한 시스템의 구조에서도 동작할 수 있는 방법으로 스크램블링부(47) 및 디스크램블링부(51)가 동작하는 시점에 대한 동기정보를 스크램블링부(47)에서 암호화된 신호를 전송하기에 앞서 동기신호 전송부(49)에서 제 2 스위칭부(48)를 통해 유선채널을 통해 전송하는 것이다.

<64> 또한 이와 병행하여 유선채널(D)로부터 수신되는 동기정보를 먼저 검출한 후, 동기정보가 검출되면, 수신된 암호화된 신호를 디 스크램블링부(51)에서 상기한 바와 같은 해독방법에 의해 해독하는 것이다. 따라서, 유선채널상에서 전송측 보코더와 수신측 보코더간의 통신신호 전송지연으로 발생하는 스크램블링부(47)와 디스크램블링부(51)의 구동시점에 대한 불일치를 해결할 수 있으며, 동일 암호키를 이용한 통신호의 암호화 및 암호화된 신호의 해독기능을 정확하게 수행할 수 있게 되는 것이다. 이때, 상기 동기정보는 미리 약속된 일정 패턴으로 구성된다.

<65> 이하, 첨부된 도 5를 참조하여 본 발명에 따른 이동통신 시스템의 음성/데이타 암호화방법 및 복호화방법을 각각 구분하여 단계적으로 살펴보는데, 먼저, 도 5a를 참조하여 이동통신시스템에서 음성/데이타 암호화방법에 대하여 살펴보기로 하자.

<66> 도 5a는 본 발명에 따른 이동통신 시스템의 보코딩장치에서 음성 및 데이타 암호화방법에 대한 동작 플로우 챠트를 나타낸 도면이다.

<67> 먼저, 무선채널 구간에서 전송되어온 음성 패킷 또는 데이타 패킷을 상위 프로세서(30)에서 제공되는 동작 모드에 따라 해당 모드를 수행한다(S101). 즉, 수신되는 음성 패킷을 지공되는 동작 모드에 따라 보코딩하여 PCM으로 변환하거나, 음성패킷을 바이패스시키거나, 또는 데이타 패킷을 바이스패스시킨다.

<68> 이어, 상위 프로세서(30)로 부터 제공되는 암호화키 정보에 따라 임의의 일정한 랜덤 넘버를 발생한다(S102).

<69> 이어, 제공되는 제어신호에 따라 동기신호를 발생하여 발생된 동기신호를 유선채널 구간으로 전송한 후(S103), 동기신호가 전송되면 상기 발생한 랜덤 넘버를 이용하여 상기 모드 처리된 신호(PCM 또는 바이패스된 음성패킷 또는 바이패스된 데이타 패킷)을 암호화한다(S104).

<70> 이렇게 암호화된 신호를 유선채널구간으로 전송하는 것이다(S105).

<71> 그리고, 도 5b를 참조하여 유선 채널구간에서 전송되어온 암호화된 신호를 해독하는 방법에 대하여 단계적으로 설명해 보기로 하자.

<72> 도 5b는 본 발명에 따른 이동통신 시스템의 보코딩장치에서 음성 및 데이타 복호화방법에 대한 동작 플로우 챠트를 나타낸 도면이다.

<73> 먼저, 유선채널 구간으로 부터 암호화된 신호를 수신되는지를 판단한다(S201).

<74> 판단결과, 암호화된 신호를 수신되면, 수신된 암호화된 신호에서 동기신호를 검출하게 되고(S202), 동기신호가 검출되는지를 판단한다(S203).

<75> 만약 동기신호가 검출되면, 제공되는 해독키에 의해 임의의 일정한 랜덤넘버를 발생한다(S204).

<76> 이어, 상기 발생된 랜덤넘버에 의해 상기 수신된 암호화된 신호를 해독(Descrambling)를 한 후(S205), 해독된 신호 즉, PCM 또는 패킷을 제공되는 동작모드에 의해 해당 모드를 수행한 후, 모드 처리된 패킷을 무선채널구간으로 전송하는 것이다(S206). 여기서, 해당 모드는 해독된 PCM을 페킷으로 변환하거나, 또는 해독된 패킷을 바이패스시키는 동작을 나타낸다.

【발명의 효과】

<77> 상술한 바와 같은 본 발명에 따른 이동통신 시스템의 음성/데이타 암호화/복호화장치 및 그 방법은 무선채널구간에서 전송되어온 신호를 보코딩 또는 바이패스시킨 후, 보코딩 또는 바이패스된 신호를 랜덤넘버를 이용하여 스크램블링하여 유선채널 구간으로 전송하고, 유선채널 구간으로 부터 수신되는 스크램블링된 신호를 동기신호의 검출 유무에 따라 상기 랜덤넘버에 따라 디스크램블링한 후, 보코딩 또는 바이패스시켜 무선채널 구간으로 전송하는 것으로서, 기존의 상용 이동통신 시스템에서 추가적인 하드웨어 변경없이 소프트웨어의 변경만으로 구현 가능한 장점이 있으며, 시스템 보코더간 유선채널 구간에서의 보안성을 획기적으로 유지시켜 도청을 미연에 방지할 수 있는 이점이 있다.

<78> 또한, 향후, 이동단말기와 보코더간의 무선채널 구간까지 확장하여 전 채널상에서 보안성을 보장할 수 있는 효과를 가진 것이다.

【특허청구범위】

【청구항 1】

이동통신 시스템의 음성/데이타 보코딩장치에 있어서,

무선채널 구간으로 부터 전송되어 온 음성/데이타 패킷을 제공되는 동작 모드신호에 따라 보코딩하거나 바이패스시키는 동작 모드 처리부와;

공급되는 암호화키에 따라 랜덤넘버를 발생시키는 랜덤넘버 발생부와;

제공되는 제어신호에 따라 동기신호를 발생하여 유선채널 구간으로 전송하는 동기신호 전송부와;

상기 랜덤넘버 발생부에서 발생된 랜덤넘버를 이용하여 상기 동작 모드 처리부에서 보코딩 또는 바이패스된 PCM 또는 음성/데이타패킷을 암호화한 후, 상기 동기신호의 전송이 완료되면, 유선채널 구간으로 전송하는 암호화부와;

상기 동작 모드 제어신호, 암호화키 공급 제어신호 및 상기 동기신호 발생 제어신호를 제공하는 제어부로 구성됨을 특징으로 하는 이동통신 시스템의 음성 및 데이타 암호화장치.

【청구항 2】

제 1 항에 있어서,

상기 제어부의 제어신호에 따라 동기신호발생부로 스위칭되어 발생된 동기신호를 유선채널구간으로 전송한 후, 동기신호의 전송이 완료되면 제공되는 제어신호에 따라 상기 암호화부로 스위칭되어 암호화된 신호를 유선채널 구간으로 전송하는 스위칭부를 더

구비하는 것을 특징으로 하는 이동통신 시스템의 음성 및 데이타 암호화장치.

【청구항 3】

제 1 항에 있어서,

상기 제어부의 제어신호에 따라 저장된 암호화키를 상기 랜덤 넘버 발생부로공급하는 안호화키 공급부를 더 구비하는 것을 특징으로 하는 이동통신 시스템의 음성 및 데이타 암호화방법.

【청구항 4】

제 1 항에 있어서,

상기 랜덤넘버 발생부에서 발생한 랜덤 넘버는 상기 동작 모드 처리부에서 보코딩된 PCM 또는 바이패스된 음성/데이타 패킷데이타를 암호화하기 위한 임의의 위치정보인 것을 특징으로 하는 이동통신 시스템의 음성/데이타 암호화장치.

【청구항 5】

이동통신 시스템의 음성 및 데이타 보코딩장치에 있어서,

유선채널 구간으로 부터 전송되어 온 암호화된 신호에서 동기신호를 검출하는 동기신호 검출부와;

제공되는 복호화키에 따라 랜덤넘버를 발생하는 랜덤넘버 발생부와;

제공되는 복호화 제어신호에 따라 상기 랜덤넘버 발생부에서 발생한 랜덤넘버에 따라 유선채널로 부터 수신된 암호화된 신호를 복호화하는 복호화부와;

상기 동기신호 검출부에서 동기신호가 검출되면, 상기 복호화부에 복호화 제어신호를 제공하고, 상기 복호화키를 공급할 수 있도록 제어신호를 제공하는 제어부와;

제공되는 동작모드에 따라 상기 복호화부에서 복호화된 PCM을 보코딩하여 패킷으로 변환하거나 또는 음성/데이타 패킷을 그대로 바이패스시킨 후, 무선채널 구간으로 전송하는 동작 모드 처리부로 구성됨을 특징으로 하는 이동통신 시스템의 음성/데이타 복호화장치.

【청구항 6】

제 5 항에 있어서,

상기 제어부에서 제공되는 제어신호에 따라 유선채널로 부터 전송되어온 암호화된 신호를 상기 복호화부로 스위칭하는 스위칭부를 더 구비하는 것을 특징으로 하는 이동통신 시스템의 음성 및 데이타 복호화장치.

【청구항 7】

제 5 항에 있어서,

상기 제어부의 제어신호에 따라 저장된 암호화키를 상기 랜덤 넘버 발생부로공급하는 복호화키 공급부를 더 구비하는 것을 특징으로 하는 이동통신 시스템의 음성 및 데이

타 암호화방법.

【청구항 8】

제 5 항에 있어서,

상기 랜덤넘버 발생부에서 발생한 랜덤 넘버는 상기 유선 채널 구간으로 부터 수신한 PCM 또는 음성/데이타 패킷데이타를 복호화하기 위한 임의의 위치정보인 것을 특징으로 하는 이동통신 시스템의 음성/데이타 암호화장치.

【청구항 9】

이동통신 시스템의 음성/데이타 보코딩장치에 있어서,

무선채널 구간으로 부터 전송되어 온 음성/데이타 패킷을 제공되는 동작 모드신호에 따라 보코딩하거나 바이패스시키고, 복호화된 PCM 또는 패킷을 제공되는 동작 모드에 따라 보코딩 또는 바이패스시켜 무선채널 구간으로 전송하는 동작 모드 처리부와;

공급되는 암호화 및 복호화키에 따라 랜덤넘버를 발생시키는 랜덤넘버 발생부와;

제공되는 제어신호에 따라 동기신호를 발생하여 유선채널 구간으로 전송하는 동기신호 전송부와;

상기 랜덤넘버 발생부에서 발생된 랜덤넘버를 이용하여 상기 동작 모드 처리부에서 보코딩 또는 바이패스된 PCM 또는 음성/데이타패킷을 암호화한 후, 상기 동기신호의 전송이 완료되면, 유선채널 구간으로 전송하는 암호화부와;

유선채널 구간으로 부터 전송되어 온 암호화된 신호에서 동기신호를 검출하는 동기신호 검출부와;

제공되는 복호화 제어신호에 따라 상기 랜덤넘버 발생부에서 발생한 랜덤넘버에 따라 유선채널로 부터 수신된 암호화된 신호를 복호화하는 복호화부와;

상기 동기신호 검출부에서 동기신호가 검출되면, 상기 복호화부에 복호화 제어신호를 제공하고, 상기 암호화키 및 복호화키를 공급할 수 있도록 제어신호를 제공하고, 상기 동기신호 발생 제어신호를 제공하는 제어부로 구성됨을 특징으로 하는 이동통신 시스템의 음성 및 데이타 암호화/복호화장치.

【청구항 10】

제 9 항에 있어서,

상기 랜덤넘버 발생부에서 발생한 랜덤 넘버는 상기 유선 채널 구간으로 부터 수신한 PCM 또는 음성/데이타 패킷데이타를 복호화하기 위한 임의의 위치정보 및 우선 채널 구간으로 부터 전송되어온 패킷을 암호화하기 위한 임의의 위치정보인 것을 특징으로 하는 이동통신 시스템의 음성 및 데이타 암호화/복호화장치.

【청구항 11】

제 9 항 또는 제 10 항에 있어서,

상기 랜덤 넘버 발생부에서 발생되는 랜덤넘버는 암호화 및 복호화시 서로 동일한 랜덤 넘버를 발생하는 것을 특징으로 하는 이동통신 시스템에서 음성/데이타 암호화 및

복호화장치.

【청구항 12】

제 9 항에 있어서,

상기 제어부의 제어신호에 따라 저장된 암호화키 및 복호화키를 상기 랜덤 넘버 발생부로 공급하는 복호화키 공급부를 더 구비하는 것을 특징으로 하는 이동통신 시스템의 음성 및 데이타 암호화/복호화방법.

【청구항 13】

이동통신 시스템의 음성 및 데이타 보코딩 방법에 있어서,

무선채널 구간에서 전송되어온 음성 패킷 또는 데이타 패킷을 제공되는 동작 모드에 따라 보코딩 또는 바이패스시킨 후, 출력하는 단계와;

제공되는 암호화키 정보에 따라 임의의 일정한 랜덤 넘버를 발생하는 단계와;

제공되는 제어신호에 따라 동기신호를 발생하여 발생된 동기신호를 유선채널 구간으로 전송하는 단계와;

상기 동기신호가 전송되면 상기 발생한 랜덤 넘버를 이용하여 상기 모드 처리된 신호(PCM 또는 바이패스된 음성패킷 또는 바이패스된 데이타 패킷)을 암호화한 후, 암호화된 신호를 유선채널구간으로 전송하는 단계로 이루어짐을 특징으로 하는 이동통신 시스템에서 음성 및 데이타 암호화방법.

【청구항 14】

이동통신 시스템에서 음성 및 데이타 보코딩방법에 있어서,

유선채널 구간으로 부터 암호화된 신호를 수신하는 단계와;

암호화된 신호가 수신되면, 수신된 암호화된 신호에서 동기신호를 검출하는 단계와;

동기신호가 검출되면, 제공되는 복호화키에 의해 임의의 일정한 랜덤넘버를 발생하는 단계와;

상기 발생된 랜덤넘버에 의해 상기 수신된 암호화된 신호를 복호화하는 단계와;

상기 복호화된 PCM 또는 패킷을 제공되는 동작모드에 의해 보코딩 또는 바이패스시켜 패킷으로 변환한 후, 무선채널구간으로 전송하는 단계로 이루어짐을 특징으로 하는 이동통신 시스템에서의 음성 및 데이타 복호화방법.

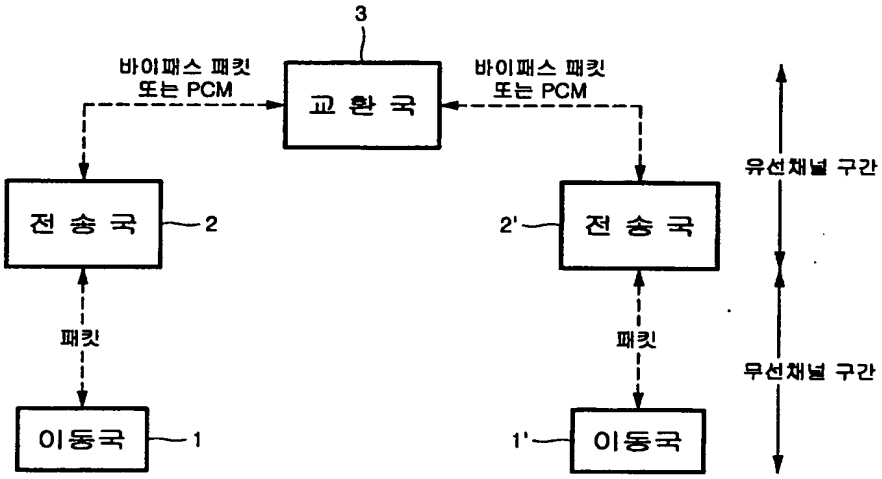
【청구항 15】

제 13 항 또는 제 14 항에 있어서,

상기 암호화 및 복호화시 발생되는 랜던넘버는 서로 동일한 랜던 넘버인 것을 특징으로 하는 이동통신 시스템에서 음성 밑 데이타 암호화/복호화방법.

【도면】

【도 1】


3
바이패스 패킷
또는 PCM
교 환 국
바이패스 패킷
또는 PCM
유선채널 구간
전 송 국
2
2'
전 송 국
패킷
패킷
무선채널 구간
이동국
1
1'
이동국

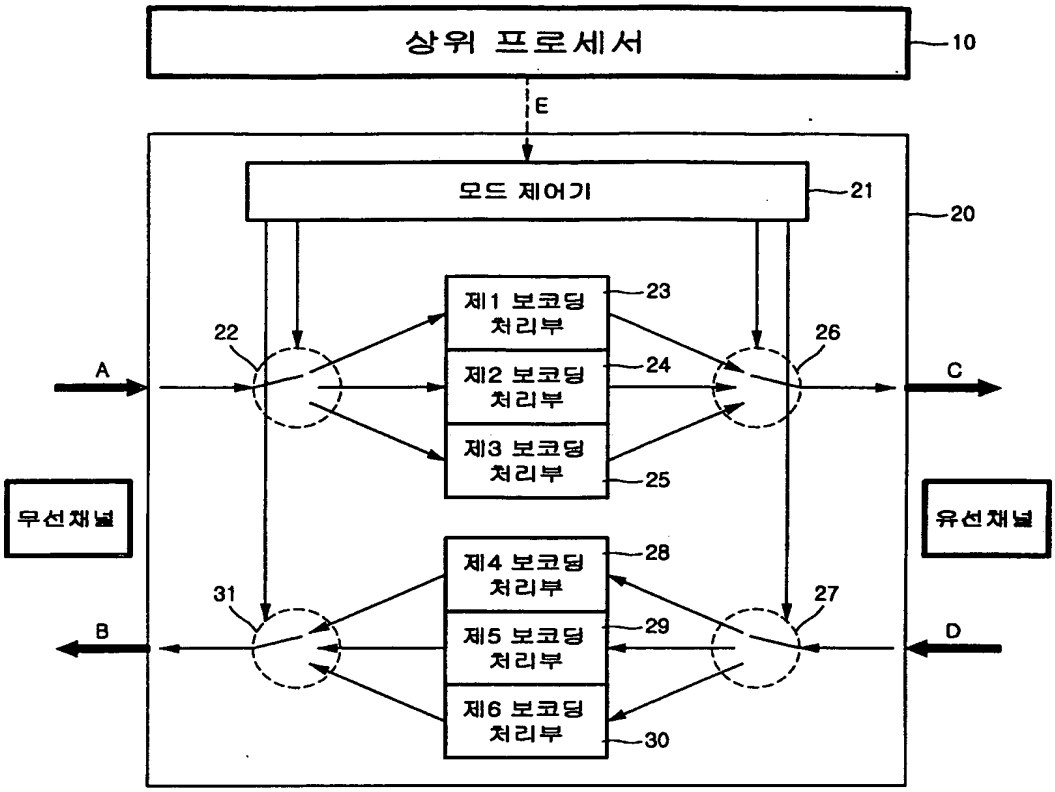
【도 2a】


Preamble
Message Header
Voice Packet
Dummy
CRC

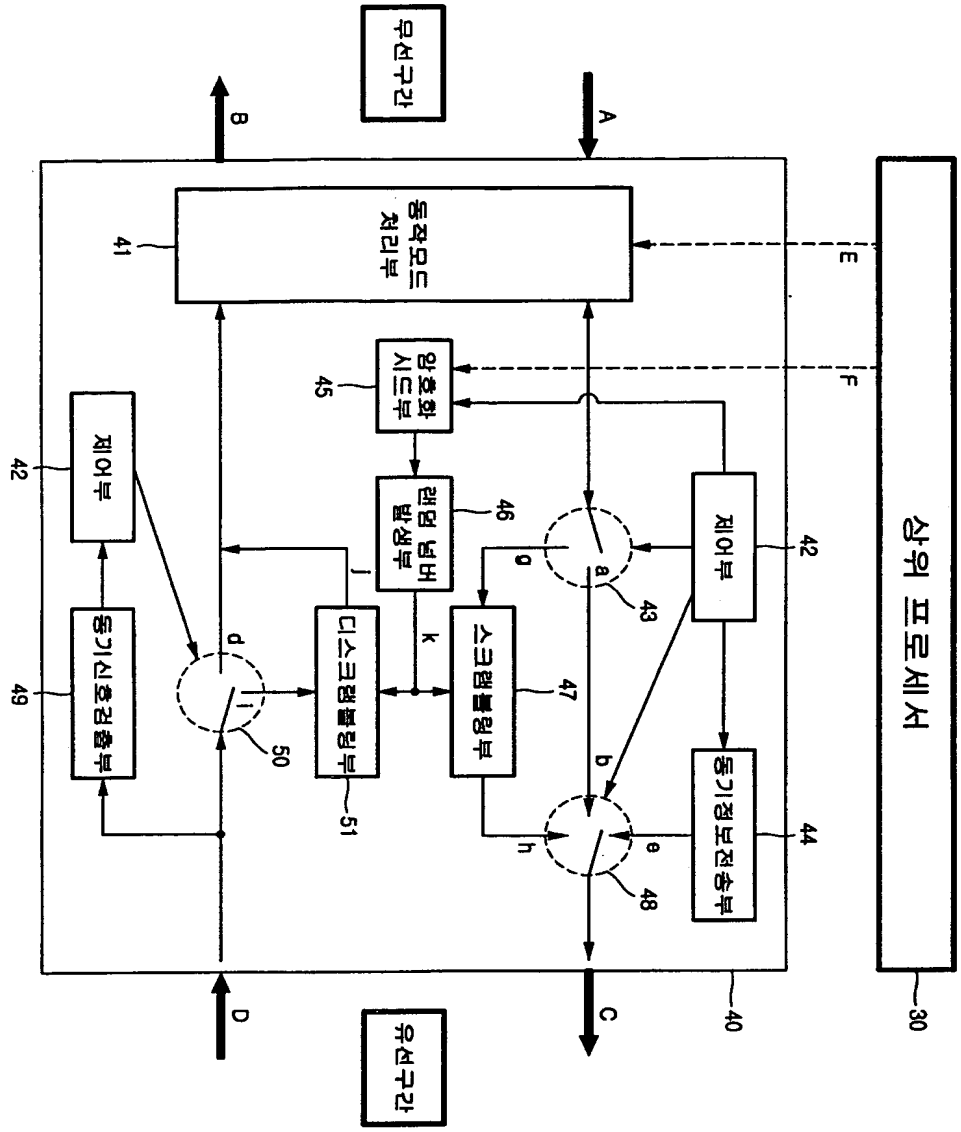
【도 2b】


Flag
Data Packet
Flag

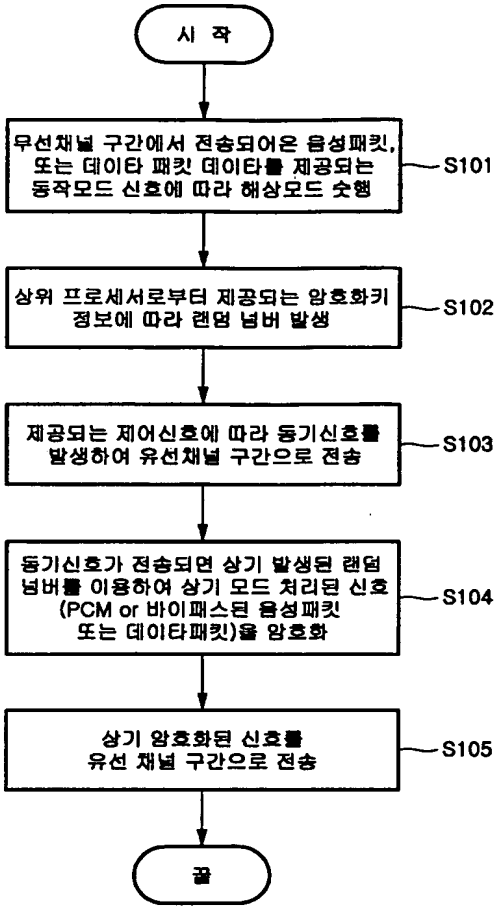
【도 3】


상위 프로세서
10
E
모드 제어기
21
20
제1 보코딩 처리부
23
22
26
A
제2 보코딩 처리부
24
C
제3 보코딩 처리부
25
무선채널
유선채널
제4 보코딩 처리부
28
31
27
B
제5 보코딩 처리부
29
D
제6 보코딩 처리부
30

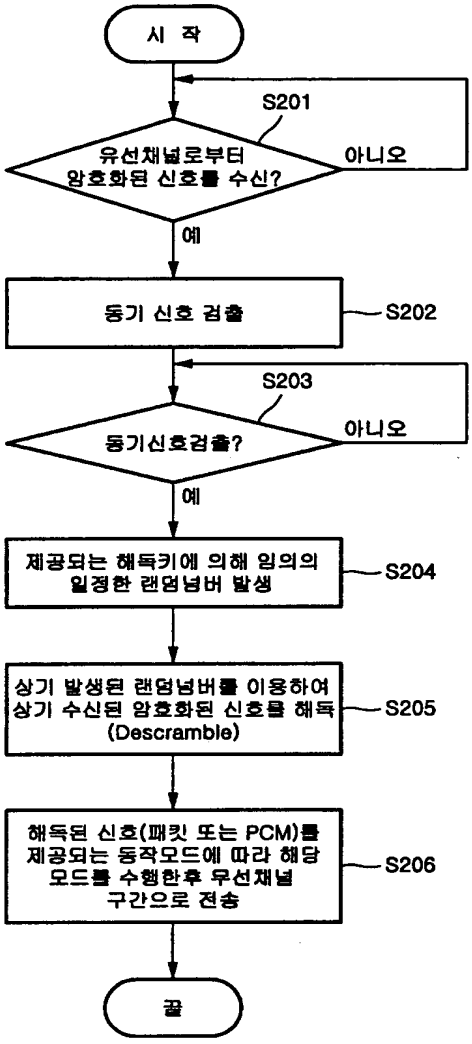
【도 4】


유선구간
B
A
동작모드 처리부
41
E
F
암호화 시드부
45
제어부
42
랜덤 넘버 발생부
46
제어부
42
상위 프로세서
동기신호검출부
49
디스크램블링부
51
스크램블링부
47
동기정보전송부
44
50
43
48
D
C
유선구간
40
30

【도_5a】


시 작
무선채널 구간에서 전송되어온 음성패킷, 또는 데이타 패킷 데이타를 제공되는 동작모드 신호에 따라 해상모드 수행
S101
상위 프로세서로부터 제공되는 암호화키 정보에 따라 랜덤 넘버 발생
S102
제공되는 제어신호에 따라 동기신호를 발생하여 유선채널 구간으로 전송
S103
동기신호가 전송되면 상기 발생된 랜덤 넘버를 이용하여 상기 모드 처리된 신호 (PCM or 바이패스된 음성패킷 또는 데이타패킷)을 암호화
S104
상기 암호화된 신호를 유선 채널 구간으로 전송
S105
끝

【도 5b】


시 작
S201
유선채널로부터 암호화된 신호를 수신?
아니오
예
동기 신호 검출
S202
S203
동기신호검출?
아니오
예
제공되는 해독키에 의해 임의의 일정한 랜덤넘버 발생
S204
상기 발생된 랜덤넘버를 이용하여 상기 수신된 암호화된 신호를 해독 (Descramble)
S205
해독된 신호(패킷 또는 PCM)를 제공되는 동작모드에 따라 해당 모드를 수행한후 무선채널 구간으로 전송
S206
끝